Amendments to the Claims:

This listing of claims will replace all prior versions, and listings, of claims in the application:

Listing of Claims:

Claims 1 to 35 (cancelled).

Claim 36 (previously presented): An information processing device comprising:

a processor;

a recording medium interface configured to read data from an information recording medium which stores data in increments of:

(a)   a first content management unit which includes first encrypted data that is encrypted by a first unit key that is set as a first encryption key; and

(b)   a second content management unit which includes second encrypted data that is encrypted by a second unit key that is set as a second, different encryption key; and

a memory device storing instructions which when executed by the processor, cause the processor to:

(a)   record new data which is either generated or obtained applying information obtained from the information recording medium;

(b)   obtain at least one of:

    (i)   the first unit key, the first unit key corresponding to the first content management unit to which the obtained information belongs; and

    (ii)   a third, different unit key which corresponds to a third, different content management unit to which the obtained information does not belong;

(c)   in response to the first unit key being obtained:

    (i)   encrypt the new data applying the obtained first unit key; and

    (ii)   execute recording processing with said encrypted new data as data configuring the first content management unit; and

(d)   in response to the third, different unit key being obtained:

    (i)   encrypt the new data applying the obtained third, different unit key; and

    (ii)   execute recording processing with the encrypted new data as data configuring the third, different content management unit.

Claim 37 (previously presented): The information processing device of Claim 36, wherein the instructions, when executed by the processor, cause the processor to:

    (a)   set a fourth content management unit corresponding to the new data; and

    (b)   execute setting processing for a third encryption key serving as management information corresponding to the fourth content management unit including the new data.

Claim 38 (previously presented): The information processing device of Claim 36, wherein the data processing unit is configured to:

    (a)   set a fifth content management unit corresponding to the new data; and

    (b)   execute setting processing for content usage control information serving as management information corresponding to the fifth content management unit including the new data.

Claim 39 (previously presented): The information processing device of Claim 36, wherein the instructions, when executed by the processor, cause the processor to execute writing processing of the new data to a region stipulated by a program included in the information obtained from the information recording medium.

Claim 40 (previously presented): The information processing device of Claim 36, wherein the instructions, when executed by the processor, cause the processor to, in a case of storing the new data in storage means other than an information recording medium from which the obtained information has been obtained, execute processing for storing the new data correlated with identification information of the information recording medium from which the obtained information has been obtained.

Claim 41 (previously presented): The information processing device of Claim 36, wherein the instructions, when executed by the processor, cause the processor to:

    (a)   execute encryption processing of an AV stream data file including new data and a navigation file including control information or a program to be applied to playing processing of the AV stream data; and

    (b)   execute recording processing of new data to storage means.

Claim 42 (previously presented): The information processing device of Claim 41, wherein the instructions, when executed by the processor, cause the processor to apply a unit key corresponding to a sixth content management unit as a fourth encryption key to be applied to the encryption processing.

Claim 43 (previously presented): The information processing device of Claim 41, wherein the instructions, when executed by the processor, cause the processor to execute encryption processing applying, as an encryption key or encryption key generating information, information which can only be obtained by an application licensed to execute processing regarding the first content management unit or the third, different content management unit.

Claim 44 (previously presented): The information processing device of Claim 43, wherein the information which can only be obtained by a licensed application is information including a device ID as an identifier unique to the device in which the application is installed.

Claim 45 (previously presented): The information processing device of Claim 36, wherein the instructions, when executed by the processor, cause the processor to:

    (a)   generate a hash value for tampering verification with regard to at least one of an AV stream data file including new data, and a navigation file including control information or a program to be applied to playing processing of the AV stream data; and

    (b)   record the hash value in a storage means.

Claim 46 (previously presented): The information processing device of Claim 45, wherein the instructions, when executed by the processor, cause the processor to:

(a) execute data tampering verification processing based on the hash value set for an AV stream data file including new data or a navigation file, at the time of using the file; and

(b) execute usage processing of the files under the condition that there is no tampering.

Claim 47 (previously presented): The information processing device of Claim 36, wherein the instructions, when executed by the processor, cause the processor to execute recording processing of a navigation file, including control information or a program to be applied to playing processing of AV stream data including new data, to storage means, as a file to which an electronic signature has been appended for tampering verification.

Claim 48 (previously presented): The information processing device of Claim 47, wherein the instructions, when executed by the processor, cause the processor to:

(a) execute data tampering verification processing based on the electronic signature set for AV stream data file including new data or the navigation file, at the time of using the file; and

(b) execute usage processing of the files under the condition that there is no tampering.

Claim 49 (previously presented): A method of operating an information processing device including instructions, the method comprising:

(a)   causing a processor to execute the instructions to read data from an information recording medium which stores data in increments of:

    (i)   a first content management unit which includes first encrypted data that is encrypted by a first unit key that is set as a first encryption key; and

    (ii)   a second content management unit which includes second encrypted data that is encrypted by a second unit key that is set as a second, different encryption key;

(b)   causing the processor to execute the instructions to record new data which is either generated or obtained applying information obtained from the information recording medium;

(c)   causing the processor to execute the instructions to obtain at least one of:

    (i)   the first unit key, the first unit key corresponding to the first content management unit to which the obtained information belongs; and

    (ii)   a third, different unit key which corresponds to a third content management unit to which the obtained information does not belong;

(d)   in response to the first unit key being obtained:

    (i)   causing the processor to execute the instructions to encrypt the new data applying the obtained first unit key; and

    (ii)   causing the processor to execute the instructions to execute processing with said encrypted new data as data configuring the first content management unit; and

(e)   in response to the third, different unit key being obtained:

    (i)   causing the processor to execute the instructions to encrypt the new data applying the obtained third, different unit key; and

    (ii)   causing the processor to execute the instructions to execute recording processing with the encrypted new data as data configuring the third, different content management unit.

Claim 50 (previously presented): The method of Claim 49, which includes:

(a)   causing the processor to execute the instructions to set a fourth content management unit corresponding to the new data; and

(b)   causing the processor to execute the instructions to execute setting processing for an encryption key serving as management information corresponding to the content management unit including the new data.

Claim 51 (previously presented): The method of Claim 49, which includes:

(a)   causing the processor to execute the instructions to set a fifth content management unit corresponding to the new data; and

(b)   causing the processor to execute the instructions to execute setting processing for content usage control information serving as management information corresponding to the fifth content management unit including the new data.

Claim 52 (previously presented): The method of Claim 49, which includes causing the processor to execute the instructions to execute writing processing of the new data to a region stipulated by a program included in the information obtained from the information recording medium.

Claim 53 (previously presented): The method of Claim 49, which includes in a case of storing the new data in storage means other than an information recording medium from which the obtained information has been obtained, causing the processor to execute the instructions to execute processing for storing the new data correlated with identification information of the information recording medium from which the obtained information has been obtained.

Claim 54 (previously presented): The method of Claim 49, which includes:

(a) causing the processor to execute the instructions to execute encryption processing of an AV stream data file including new data and a navigation file including control information or a program to be applied to playing processing of the AV stream data; and

(b) causing the processor to execute the instructions to execute recording processing of new data to storage means.

Claim 55 (previously presented): The method of Claim 54, which includes applying a unit key corresponding to a content management unit as an encryption key to be applied to the encryption processing.

Claim 56 (previously presented): The method of Claim 54, which includes applying, as an encryption key or encryption key generating information, information which can only be obtained by an application licensed to execute processing regarding the content management unit.

Claim 57 (previously presented): The method of Claim 56, which includes wherein the information which can only be obtained by a licensed application is information including a device ID as an identifier unique to the device in which the application is installed.

Claim 58 (previously presented): The method of Claim 49, which includes:

(a) causing the processor to execute the instructions to generate of a hash value for tampering verification with regard to at least one of an AV stream data file including new data, and a navigation file including control information or a program to be applied to playing processing of the AV stream data; and

(b) causing the processor to execute the instructions to record of the hash value in storage means.

Claim 59 (previously presented): The method of Claim 58, which includes:

(a)   causing the processor to execute the instructions to execute data tampering verification processing based on the hash value set for the AV stream data file including new data or the navigation file, at the time of using the file; and

(b)   causing the processor to execute the instructions to execute usage processing of the files under the condition that there is no tampering.

Claim 60 (previously presented): The method of Claim 49, which includes causing the processor to execute the instructions to execute recording processing of a navigation file, including control information or a program to be applied to playing processing of AB stream data including new data, to storage means, as a file to which an electronic signature has been appended for tampering verification.

Claim 61 (previously presented): The method of Claim 60, which includes causing the processor to execute the instructions to execute data tampering verification processing based on the electronic signature set for the AV stream data file including new data or the navigation file, at the time of using the file, and executing of usage processing of the files under the condition that there is no tampering.

Claim 62 (currently amended): A ~~computer readable medium~~ non-transitory machine-accessible and readable storage medium storing instructions structured to cause an information processing device to:

(a)   read data from an information recording medium which stores data in increments of:

    (i)   a first content management unit which includes first encrypted data that is encrypted by a first unit key that is set as a first encryption key; and

    (ii)   a second content management unit which includes second encrypted data that is encrypted by a second unit key that is set as a second, different encryption key; and

(b)   record new data which is either generated or obtained applying information obtained from the information recording medium;

(c)   obtain at least of:

    (i)   the first unit key, the first unit key corresponding to the first content management unit to which the obtained information belongs; and

    (ii)   a third, different unit key which corresponds to a third, different content management unit to which the obtained information does not belong;

(d)   in response to the first unit key being obtained:

    (i)   encrypt the new data applying the obtained first unit key; and

    (ii)   execute recording processing with said encrypted new data as data configuring the first content management unit; and

(e)   in response to the third, different unit key being obtained:

    (i)   encrypt the new data applying the obtained third, different unit key; and

    (ii)   execute recording processing with the encrypted new data as data configuring the third, different content management unit.

Claim 63 (currently amended): The ~~computer readable medium~~ non-transistory machine-accessible and readable storage medium of Claim 62, wherein the instructions are further structured to cause the information processing device to:

    (a)   encrypt an AV stream data file including new data, and a navigation file including control information or a program to be applied to playing processing of AV stream data including new data; and

    (b)   execute recording to recording means.

Claim 64 (currently amended): The ~~computer readable medium~~ non-transistory machine-accessible and readable storage medium of Claim 62, wherein the instructions are further structured to cause the information processing device to:

    (a)   record, to storage means, tampering verification data regarding at least one of an AV stream data file including new data, and a navigation file including control information or a program to be applied to playing processing of AV stream data including new data; and

    (b)   execute recording to recording means.

Claim 65 (currently amended): The ~~computer readable medium~~ non-transistory machine-accessible and readable storage medium of Claim 62, wherein the instructions are further structured to cause the information processing device to:

    (a)   execute data tampering verification processing based on the tampering verification data set for the AV stream data file including new data or the navigation file, at the time of using the file; and

    (b)   execute usage processing of the files under the condition that there is no tampering.